Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 58 (2015) 643 – 648

Procedia Computer Science

Second International Symposium on Computer Vision and the Internet(VisionNet'15)

Design and Development of Algorithm Using Chemical Cryptography

Prof(Dr.) Amit Verma[a], Anjali Gakhar[b]*

*Professor, Chandigarh University, Mohali 140413, India
*Student, Chandigarh University, Mohali 140413, India

Abstract

According to the present network scenario security is one of the main concerns. Secure communication disentitles the third party to listen or copy the same unauthorizedly. The word cryptography comes from the Greek language but is being employed by varieties of nations. The process of hiding the information or talking in codes is not a new task, it's always been used by every person who is surrounded by us. In the present paper a new approach is focused that ensures the security of the information, but before various tools and techniques are going to be discussed that were used in the past and some of them were employed in the wars. After the discussion there is a comparative study that consists of the comparative analysis of ciphers and techniques with respect to their eras.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)

Keywords: Claude Shannon; OTP; Aborgeneis;Enigma;Ceyptosystem; Chemical Cryptography;

1. Introduction

When communication takes place between two persons, they always want that their talk should be kept [1] secret. Third entity present in the network tries to break the secrecy of the system and always try to break the authentication integrity and confidentiality. To attain the confidentiality of the message the two communicating parties always use varieties of cryptographic tools and techniques that help them to communicate securely and must satisfy three goals:-

Table 1Goals of Security [4]

Goals	Description	Attacks
C_Y	Information within the n/w should be confident. Only Source and sink know about it.	$R_{MC.}$;T.A
I_Y	Information should not be modified or altered. I_Y should be maintained.	I_{TP} ;M_{DF}
A_Y	Ensures that communication takes between the claimed parties.	F_{BN}

*Anjali Gakhar. Tel.:09416239775; fax: +0-000-000-0000 .
E-mail address:anjaligakhar7@gmail.com.

Peer-review under responsibility of organizing committee of the Second International Symposium on Computer Vision and the Internet (VisionNet'15)
doi:10.1016/j.procs.2015.08.083

Where, *C_Y: Confidentiality, *I_Y: Integrity, *A_Y: Availability, *R_{MC}: Release of message content; *I_{TP}: Interruption; *M_{DF}: Modification, *F_{BN}: Fabrication; T.A: Traffic Analysis;

The above table is showing the CIA of security that prevents the information from the various unauthorized attempts. While moving forward to the concept of security some of the terms should be known for understanding the concepts.

1.1. Terminology

When information is sent from source to sink it should always be in [3] encrypted form and encryption can be done through various algorithms and at the receiver side same procedure is done for getting the required plain text. Here are some of the key terms in the following table:

Table 2 Related Terms [6,8]

Keywords	Description
P.T	Original message, easy to read and understand.
C.T	Covert Message, Scrambled, not understandable and encrypted with key.
K (P_{UK}, P_{RK})	• Public Key: - Consists of a pair of keys. One is used for encryption on the sender side and other is used for decryption on the receiver side. • Private Key: A single key used for both encryption and decryption.
E_A	An algorithm that is used to encode the plain text with the help of the key.
D_A	It is a reverse process of encryption algorithm held at the receiver side.

Where, *P.T: Plain Text; *C.T: Cipher Text; *K: Key; *P_{UK}; Public Key;* P_{RK}: Private Key;* E_A: Encryption Algorithm; *D_A: Decryption Algorithm;

The message originated [5] from source side and received at the other end of the side of the network. While in sending and receiving of the message two conversions take place, known as the process of encryption and decryption. The following two equations take place: -

For generating Cipher Text, C.T→"EA (P.T)" Conversion done at Source → (1)

For generating Plaint Text, P.T→"DA (C.T)" Conversion done at Sink → (2)

The Concept of cryptography used in various countries and at various positions. According to the literature, it was first originated at the stone age where people started there communication using the hand movements while hunting. The next section consists of various previous techniques that were used in past with the aim of achieving high security.

2. Previous Techniques

Cryptography, the art or technique of enciphering and deciphering the message in a secret code has played and still playing vital roles in the history of every nation. It is becoming a necessary step in this crazy world where there is fight among the code makers and code breakers. From [18, 19]1900 B.C the process of cryptology was initiated by the Egyptian scribe while attempting to maintain the records in their own language. They made use of the non standard hieroglyphics for communication purpose. It was the first attempt and after this in 1500 B.C one more attempt was made in Mesopotamia, where a miniature encipher flap was found that was enclosed with the veiled the formula for glazing pottering. Cryptography is not limited to an individual or to a group of individuals; it serves the whole world for keeping their information secure from others. The use of cryptography is mounting day by day; it is being employed in wars and used in many organizations. The cryptosystem consists of 5 tuples (***O, C, K, E, D***), [9] that must satisfy the rule:-

Rule1: For each task there is an encryption rule $e_K \in E$ and corresponding rule $d_K \in D$ where, e_K: $O \rightarrow C$ and $d_K \in C \rightarrow O$ are functions such that $d_K (e_K (m)) = m$ for every original message $m \in O$.

Mathematical_Notation_of_Cryptosystem[9]

Cryptosystem basically has five tuples (***O, C, K,E,D***), where the following conditions are satisfied:

1. **O** is the finite set of possible originate message;
2. **C** is the finite set of possible cipher texts;
3. **K** is the finite set of possible keys;
4. ***E*** is the encryption algorithm;
5. ***D*** is the decryption algorithm;

The above mathematical notation of cryptosystem given will define the tuples with their conditions that follows *Rule1*. The cryptography is broadly divided into three main era's that is classic cryptography where enciphering is done only with the help of pen and paper, then medieval era of cryptography where various substitution and transposition came into existence and at last the modern era of cryptography where revolutionary encryption

techniques are introduced such as DES, 3DES, AES etc. Several cryptography techniques have been shown in the following table:-

Table 3 Tools and Technique of Cryptography

1. C_R	1.1 C_L	1.1.1L_G	A) N_{SH}		
			B) P_{GS}		
			C) R_U		
		1.1.2 T_Q	A) S_S	a) M_{AS}	i. CS_R
					ii. A_F
					iii. R_{13}
					iv. A_{TB}
				b) P_{GS}	
			B) T_P	a) S_{CL}	
				b) R_T	
				c) C_T	
			C) S_G	a) $P_{HY}S_G$	
	1.2 M_L	1.2.1 T_Q	A) S_S	a) P_{AS}	i. A_{LB}
					ii. V_{GN}
					iii. W_{HL}
					iv. P_F
					v. V_{RM}
				b) P_G	
				c) M_S	i. ADFGVX
		1.2.2 M/C	A) E_{GM}		
			B) P_{RP}		
	1.3 M_N		A) S_G	a) M_MS_G	i. I_MS_G
					ii. A_DS_G
		1.3.1 T_Q			iii. V_DS_G
			B) S_M	a) L_C	
				b) DES	
				c) TDES	
				d) I_D	
				a) AES	
			C) AS_K	a) Q_{TM}	
				b) RSA	

Where, *C_R: Cryptography; *C_L: Classic; *M_L: Medieval; *M_N: Modern; *L_G: Language; *T_Q: Technique; *M/C: Machine; *N_{SH}: Non Standard Hieroglyphics; *P_{GS}: Pictographs; *R_U: Runes; *S_S: Substitution; *T_P: Transposition; *M_{AS}: Monoalphabetic; *P_{GS}: Polygraphic; *S_G: Steganography; *E_{GM}: Enigma; *P_{RP}: Purple; *S_M; Symmetric; *$AS_{M:}$ Asymmetric; *CS_R: Caser; *A_F: Affine; *R_{13}: Rot13; *A_{TB}: Atbash; *S_{CL}: Scytale; *R_T: Row Transposition; *C_T: Column Transposition; *$P_{HY}S_G$: Physical Steganography; *P_{AS}: Polyalphabetic Substitution; *P_G: Polygraphic; *M_MS_G: Multimedia Steganography; *DES: Digital Encryption Standard; *AES: Advanced Encryption Standard; *Q_{TM}: Quantum; *RSA: Rivest Shamir Adelman: * A_{LB}: Alberti; * V_{GN}: Vigenere; * $W_{HL;}$ Wheel;* P_f: Playfair;*V_{RM} Vernam; *I_MS_G: Image steganography; *A_DS_G: Audio Steganography; *V_DS_G: Video Steganography; *L_C : Lucifer ; *I_D: Idea;* TDES: Triple DES

2.1. Classic Era

The classic era starts from the very past where aborigines use hand movement for the communication while hunting in 9997 B.C after that in 1900 B.C Egyptian scribe use various symbols that were carved on the rock and named as hieroglyphics. Although the previous attempt was not serious they were done only for the record keeping. After so many years a Hebrew [1] scribes introduce a new way to scramble the information. The text in the message is substituted from the previous letter so that the intruder was unable to know the actual information. This attempt was made in 50-60 B.C and easily broken after some time because of its low level of complexity. The Hebrew cipher is also known as the [9] atbash cipher that works on the principle of substitution. Here, is pseudo code of substitution technique in which current letter is substituted with the other letter.

Substitution_ Cipher

Assume $O=C=X_{26,}$ whereas K includes set of all possible permutations starting from 0 to 25.

There should be a random permutation say, Ω and belongs to K.

Encryption can be done as $E_\Omega(\alpha) = \Omega(\alpha)$, → (3)

And,

Decryption is defined as $D_\Omega(\beta) = \Omega^{-1}(\beta)$, → (4)

Where, Ω^{-1} is the inverse permutation to Ω.

Rule2: "A sequential replacement of an original message with cipher text in order to scramble every single bit of the plain text."In 50-60 B.C [7] Julius Caesar introduces one more way to scramble the message that is based on the shift technique. In his way of encrypting message current letter was replaced to the third letter that is he shifts the positions of the letter to make the text irrelevant. That is a will become d and d will become g.

Shift_ Cipher

Assume $O=C=K=X_{26,}$

For $0 \leq K \geq 25$ Perform, Encryption $E_K(\alpha) = (\alpha + K) \bmod 26, \rightarrow$ (5) &

Decryption $D_K(\beta) = (\beta - K) \bmod 26, \rightarrow$ (6)

Where, $(\alpha, \beta \in X_{26})$

A brief summary of classical ciphers is given in the following table with respect to their various features.

Table 4 Classic Era Ciphers

S_N	C_{PH}	N_{SH}	M.F	$A_{TB}\ C_{PH}$	S_G	$S_{CL}\ C_{PH}$	$P_B\ C_{PH}$	$C_R\ C_{PH}$
1	Y_R	1900 B.C	1500 B.C	500-600 B.C	440 B.C	487 B.C	205-123 B.C	50-60 B.C
2	D_{PR}	E_S	M_{PM}	H_W	H_{DS}	S_{PT}	P_B	J.C
3	E_T	UL	N_A	M_{AS}	M_H	T_P	M.S	M.S
4	K_S	N_A	N_A	N_A	N_A	L_S	N_A	N_A
5	V_L	N_S	N_A	$K.C_{TO}$	N_A	N_A	N_A	C_{TO}, B.F.A
6	C_{AT}	Civ.	Civ.	Civ.	Govt./Civ.	Civ./Govt.	Civ./Govt.	Govt.
7	S_{FT}	N_A	N_A	-1	N_A	N_A	N_A	+3
8	S_{TR}	D.S	D.S	L_R	S_{TR} of O_{BJ}	L_{PS}	5x5 M_X	Linear
9	F_Y	R_DK_P	P.I	S_{MBG}	M.H	S.M	Conv.(A→ N)	S_{MBG} via S_S

Where,* C_{PH}: Cipher; *M.F: Mesopotamian Flap; *$D_{PR:}$ Developer; $E_{T:}$ Encryption Technique; K_S: Key Size; V_L: Vulnerability; C_{AT}: Category; S_{FT}: Shifts, S_{TR}: Structure; *F_Y: Functionality; *U_L Undiscovered Language; *Civ. Civilians; *Govt.: Government; *B.F.A: Brute Force Attack; L_S: Length of Stick; L_{PS}: Length of Paper &Stick; J.C: Julius Caser; R_DK_P: Record Keeping; M_{PM}: Mesopotamians; H_W: Hebrew; H_{DS}: Herodotus; S_{PT}: Spartans; D.S: Different Shapes; S_{TR} of O_{BJ} :Structure of Object; M.H: Message Hiding; L_R: Linear; P.I: Pottery Information; S.M : Secret Messages; S_{MBG}: Scrambling; $M_{X:}$ Matrix; M_H: Message Hiding; N_A: Not Avail; *$K.C_{TO}$; Known Cipher Text only;

2.2. Medieval Era

In the medieval era of cryptography various ciphers were introduced some of them were very strong and some of them were used only for some years only. In [20, 14] this era one more cipher came into existence that promises an unconditional security. This cipher was given by Gilbert S. Vernam and the cipher works over a condition that the key that is used for encryption purpose should be pure random and of the same length of the message. Here, is a pseudo code of Vernam Cipher.

Pseudo code_ Vigenere_ Cipher

Let n be a positive integer

Assume , $O=C=K=(X_{26})^n$

For $K=(K_1 - - - K_n)$

Execute, $E_K(\alpha_1, \alpha_{2,} \alpha_{3,} - - - \alpha_n) = (\alpha_1+K, \alpha_2+K_2 - - - - \alpha_n+K_n)$, →Eq7 and

for decryption; $D_K(\beta_1, \beta_{2,} \beta_{3,} - - - - \beta_n) = (\beta_1-K_1, \beta_2-K_2, - - - - \beta_n-K_n)$ →Eq8

Where, All operations are performed in X_{26}

. Here is a comparative table that includes medieval era ciphers with their some of the characteristics.

Table 5 Medieval Era Ciphers [9, 11, 16, 20,21]

S_N	C_{PH}	A_{LB}	V_{GN}	W_{HL}	P_F	V_{RM}	ADFGVX	E_{GM} M/C
1	Y_R	1466	1585	1790	1854	1917	1918	1923
2	D_{PR}	L.B.A	B.D.V	T.J	C.W	G.S.V	F.N	A.S
3	E_T	P_AS	P_AS	P_AS	P_AS	P_AS	M.S	P_AS
4	K_S	N_A	N_A	O_W	25 K	L_M	N_A	N_A
5	C_TA_Y	$F_Q\ A_Y$	K.T	$K.C_{TO}$	$F_Q\ A_Y$	E_VD_{PG}	$M_R\ C_D$	B_B m/c
6	C_{AT}	Civ.	Civ.	Civ./Govt.	Civ.	Civ.	Govt.	Govt.
7	S_{FT}	N_A	N_A	N_A	N_A	N_A	N_A	N_A
8	S_{TR}	2 C.D	26x26 M_X	36D&A w26 A_{LP}	5x5 M_X	B.D	6x6 M_X	R_{TR}, P.B, L.B, R_{FR}
9	F_Y	Enc.	Enc.	Enc.	Enc.	Enc.	Enc.	Enc.

Where, *K.T: Kiaski Test; *O_W: Order of wheel; *L_M: Length of message;; *$M_R\ C_D$: Morse code; *B_B m/c: Bomb machine; *C.D: Concentric Disk; *R_{TR}: Rotor; *P.B: Plug Board; *L.B: Lamp Board; *R_{FR}: Reflector; *E_VD_{PG}: Eavesdropping; *D&A Disk and Axile; *B.D: Binary Digits; A_{LP}: Alphabets; * B.D.V: Blaise de Vigenere;*A.S: Arthur Scherbius;

2.3. Modern Era

Cryptography reaches to a new level with the start of modern era. The [14] modern era starts with the theory of Claude Shannon. According to him if we divide the message and then perform some permutation and combination

then the new text generated is totally different from the originate message and the method is known as the diffusion and confusion. In new ciphers the same theory is repeated over and over again to generate the complex output that is difficult to know and break. In [13] 1970 a standardized technique was given by the IBM that is based on the Fiestel structure in which total 16 rounds are performed to make the message scrambled and meaningless. The modern era ciphers are broadly divided into two categories and named as symmetric and asymmetric key encryption.

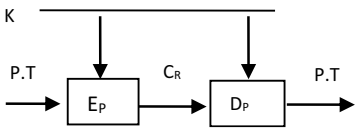

Fig1.a Symmetric encryption

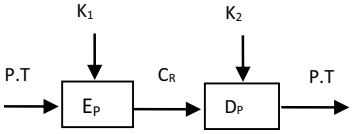

Fig1.b Asymmetric encryption

The above two figures display the basic working of two techniques in which key plays main role for encryption and decryption. [15] DES 3DES AES use only one key for encryption and decryption purpose where RSA, Quantum like cryptographic techniques uses two pair of key one for encryption and other for decryption. Here is a comparative study of modern eon ciphers with respect to some common characteristics.

Table 5 Modern Era Ciphers [12, 13, 15, 17]

S_N	C_{PH}	L_C	DES	RSA	Q_{TM}	TDES	I_D	AES
1	Y_R	1970	1997	1978	1978-13	1998	1991	2000
2	D_{PR}	H.F	IBM	R.S.A	S.W	IBM	X.L.J	R_D
3	E_T	S_K	S_K	AS_K	AS_K	S_K	S_K	S_K
4	K_S	128	56	1024	N_A	168	128	128,192,256
5	G_{RY}	B.C	B.C	N_A	N_A	B.C	B.C	B.C
6	C_{AT}	Civ.	Civ./Govt.	Civ.	Civ./Govt.	Civ.	Govt.	Civ./Govt.
7	R_{DS}	16	16	1	N_A	48	8.5	10,12,14
8	S_{TR}	F.N	F.N	PKA	N_A	F.N	L.M.S	S.P.N
9	F_Y	Enc.	Enc.	Enc.	Enc.	Enc.	Enc.	Enc.

Where, *H.F: Horst Feistel; *B.C: Block Cipher; *PKA: Public Key Architecture; *F.N Fiestel Network; *SW: Stephen Wiesner* L.M.S: Lai-Massey Scheme *X.L.J: Xuejia Lai & James Massey * R_D: Rijndeal; *S.P.N: Substitution-Permutation Network;

3. Proposed Work

Asymmetric key cryptographic schemes require high cost for implementation in comparison with symmetric key encryption; also some problems occurred while implementing the public key ciphers. In symmetric key ciphers covert message can be decoded in an unauthorized way using brute force attack or via differential and linear cryptanalysis. In this paper a new technique is proposed under the symmetric ciphers which has high key size and requires a lot of time is required to break it.

Proposed Algorithm	
Begin	Begin
{	{
Read P.T;	Read C.T;
Convert P.T → D_{CV};	Apply H.C;
Assign A_{TM} E_{LM} to D_{CV} from 99X99; matrix;	Perform D_{CV}→B_{NV};
Perform mod4;	Perform XOR;
Perform R_{DK} O_P;	Convert B_{NV} →D_{CV};
Convert D_{CV} →B_{NV};	Perform R_{DK} O_P;
Perform XOR;	Perform mod4;
Perform B_{NV}→D_{CV};	Assign A_{TM} E_{LM} to D_{CV} from 99X99 matrix;
Apply H.C;	Convert D_{CV} → P.T;
Generate C.T;	Generate P.T;
}	}
End	End

Where, *P.T: Plain Text; *D_{CV}: Decimal value; *A_{TM} E_{LM}: Atomic Element; *R_{DK} O_P: Random Key Operation; *B_{NV}: Binary Value; *H.C: Huffman Coding; C.T: Cipher Text.

The theory of Claude Shannon is followed while designing a cryptosystem. The process of diffusion and confusion is greatly and the standard 26 alphabets are replaced with 99 elements and unconditionally secure cipher OTP is used for making the cryptosystem more complex. With the increase in key the time taken to break system is increase and the brute force attack also required more time to break and according to Kirchhoff law the security of the cryptosystem depends on the privacy of the key combinations and randomization. In the proposed algorithm a

unique approach is followed that makes information highly secure and confident. Here is comparison table that will show a comparative analysis with the existing algorithms.

Table 6.1 Comparison Table

A_{GR}	K_S (BITS)	φ
M_{EA}	N_A	↓
DES	56	↔
AES	128, 256	↑
P_{RP} A_{GR}	9081	↑↑

Where∗ φ: Complexity; *P_{RP} A_{GR}: Proposed Algorithm;

With the increase of keys the computation required to break the cipher also increased. Table 6.1a and 6.1b shows the complexity level, number of alternative keys also with the time required at1 and 10 μ_S. Proposed algorithm is compared with various algorithms key size.

Table 6.2 Comparative Analysis

K_S (BITS)	φ	**N_O. A_{LT} K**	T_D/1 μ_S	T_D/10 μ_S
32	↓↓	$2^{32} = 4.3X10^9$	$2^{31} = 35.8$ min	2.15 m_S
56	↓	$2^{56} = 7.2X10^{16}$	$2^{56} = 1142$ Y_{rs}	10.81 h_{rs}
128	↔	$2^{128} = 3.4X10^{38}$	$2^{128} = 5.4X10^{24}$ Y_{rs}	$5.4X10^{18}$ Y_{rs}
168	↑	$2^{168} = 3.7X10^{56}$	$2^{168} = 5.9X10^{36}$ Y_{rs}	$5.9X10^{30}$ Y_{rs}
256	↑	$2^{256} = 3.31X10^{106}$	$2^{256} = 5.4X10^{48}$ Y_{rs}	$5.4X\ 10^{26}$ Y_{rs}
9801	↑↑	$2^{9801} = 2.1X10^{2950}$	$2^{9801} = 3.0X10^{2953}$ Y_{rs}	$3.0X10^{2947}$ Y_{rs}

Where, *No. A_{LT} K: Number of alternative keys;

4. Conclusion

The widespread use of computer technology for information handling has resulted in the need for higher data protection. The usage of high profile cryptographic protocols and algorithms do not always necessarily guarantee high security. However, choosing the right package with right security parameters can lead to a secure and best performance communication environment. Encryption and Decryption requires generating a matrix which is essentially the power of security. The use of periodic table in the security is applied for the first time. And this may lead to a new way to encrypt the message so that the task of getting the plaintext is little bit more difficult for the person who doesn't have the special knowledge. With the help of data encryption technique we can convert the plain text into cipher text so that the unauthorized person can't interrupt between the communications. Today data encryption technique is used in every sector to maintain the data integrity and make it confidential and authenticated.

5. References

1. D. Khan, "*The Code Breakers: The Story of Secret Writing*". NY: The New American Library, Inc.1973.
2. S. Singh, "*The Code Book: How To Make It, Break It, Hack It, Crack It*". Broadway, NY: Delacorate Press 2001.
3. W. Stallings, "*Network Security Essentials: Applications and Standards*".India: Pearson Publication 2003.
4. R. Bragg, M.P. Ousely and K. Strasberg, "*Data Security Architecture in Network Security: The Complete Reference*". New Delhi India: Tata McGraw-Hill 2004.
5. K.T. Fung, "*Network Security Technologies*". London NY: Auerbach Publications 2005.
6. H.C.A.V. Tilborg, *"Encyclopedia of Cryptography and Security*". Springer 2005
7. K.H. Rosen, "*Cryptography Theory and Practice*". London NY: Taylor and shift 2007
8. D.R. Stinson, "*Cryptography Theory and Practice"* .London NY: Taylor and shift 2007.
9. A. Kahate, "*Cryptography and Network Security*". India: Tata McGraw Hill Edition 2008
10. B.A. Forouzan and D. Mukhopadhyay, "*Cryptography and Network Security*". New Delhi India: Tata McGraw Hill Edition 2010.
11. A. Hodges, "*Alan Turing: The Enigma*". Princeton NJ: Princeton University Press 2014.
12. W. Diffie and M. E. Hellman "New Directions in Cryptography" IEEE Transactions on Information Theory, Vol. 22(6), pp. 644-654, November 1976.
13. M. E. Smid and D. K. Brantad "The Data Encryption standard: Past and Future", Proceedings of IEEE, VOl.76 (5), pp.550-559, May, 1998.
14. F.A.P. Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding-A survey", Proceedings of IEEE, Vol.87 (7), pp. 1062-78, July 1999.
15. Federal Information Processing Standards Publication 197"Specification for the Advanced Encryption Standard", pp 1-47, 26 November 2001.
16. L. Kruth and C. Deavours "The Commercial Enigma: Beginnings of a Machine Cryptography", Cryptologia, Vol. 46(1), pp.1-14. January 2002.
17. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography", Rev. Mod. Phys. 74, pp- 145-195, 2002
18. A Short History of Cryptography Available at "https://www.youtube.com/watch?v=H9Cu36Qj3dQ "Access on 12/28/2014.
19. Ancient Civilization available on "http://www.dl.ket.org/humanities/connections/class/ancient/index.htm" Accessed on 31/1/2015
20. www.Ciphermachines.com
21. www.cryptomuseum.com